Patented Mar. 5, 1946 2,395,863

UNITED STATES PATENT OFFICE

2,395,863

CRYPTOGRAPHIC DEVICE

William F. Friedman, Washington, D. C.

Application October 19, 1939, Serial No. 300,212

19 Claims. (Cl. 35—2)

(Granted under the act of March 3, 1883, as amended April 30, 1928; 370 O. G. 757)

The invention described herein may be manufactured and used by or for the Government for governmental purposes, without the payment to me of any royalty thereon.

This invention relates to cryptographic devices and has for its object the provision of a hand-operated device capable of affording a relatively high degree of security without involving the use of complicated mechanisms.

Another object is to provide a device useful in cryptographic and cryptanalytic investigations requiring the use of sliding alphabets.

The invention is described with reference to the accompanying drawings, in which:

Fig. 1 is a perspective showing one form or embodiment of the invention;

Fig. 2 is a top plan view of another embodiment of the invention;

Fig. 3 is a cross-section taken on the line 3—3 of Fig. 2;

Fig. 3*a* is a fragment of the same section on an enlarged scale showing the T-grip for the guide rule in operative position;

Fig. 4 is a top view of the form of invention of Fig. 1 showing the guide rule in shifted position;

Fig. 5 is a top plan view showing another embodiment of the invention in which the base is composed of separate detachable grooved sections;

Fig. 6 is a perspective showing one of the grooved sections; and

Fig. 7 is a perspective showing a frame structure and sub-base on which said grooved sections may be assembled.

Referring to Fig. 1, in this embodiment the device comprises a base 1, on which are horizontally fastened a series of cylindrical rods 2, forming a set of channel ways 3, into which character bearing strips 4, may be inserted and slid from left to right or vice versa. In the specific embodiment disclosed herein the device comprises twenty-five such channel ways, but the device is by no means limited to this number. The number chosen in this embodiment is merely a convenient number, and it may be increased or decreased within certain limits in other embodiments without materially departing from the spirit of the invention. A rule, or reading guide 5, attached to a reading guide slide 6, can be slid to the left or right on a reading guide slide rail 7. End bars 8 and 9, serve as stops against which the reading guide 5 may be brought at the end of its travel to the left or right. To the back of the base 1 is fastened a hinged support 10, which can be pulled out to support the device in a slanting position as it rests upon a table, desk, or other plane surface. Or, if the operator prefers to lay the device flat upon the table, the rubber feet 11, at the four corners of the bottom of base 1 will support the device and keep it from sliding about on the table.

As stated above, into the channel ways 3 there are inserted character strips 4 of paper or other suitable material, hereinafter called alphabet strips, upon which appear sequences of letters of the alphabet, each sequence being repeated on the strip, and the letters being equidistant from one another throughout. The purpose of the duplication of sequence will appear presently. The letters on the alphabet strips may be in normal order or in disarranged order; if the latter, the various alphabets may or may not be different. Assuming, however, different alphabets are being used, each strip bears an identifying mark such as a number 14, so that the alphabet strips may be inserted into the channel ways 3 according to some preagreed key. For example, in Fig. 1 is shown a set of twenty-five channel ways into which twenty-five different alphabet strips 4 have been inserted according to the following key, reading from the top downward:

14—16—9—6—22—25—23—5—12—24—13—21—18—1—7—17—20—19—15—8—11—2—3—10—4

If another embodiment of the device should include more than twenty-five channel ways, additional alphabet strips may be inserted, according to a longer key.

Having inserted the alphabet strips into the channel ways in key order, the device is now ready for use either to encipher a plain language message or to decipher a cryptogram which has been enciphered by means of the device, alphabets, and key shown in Fig. 1. Suppose this plain-text message is to be enciphered:

ACCORDING TO AN OFFICIAL REPORT
FROM MILITARY AUTHORITIES . . .

Moving the reading guide 5 to the left, and bringing it against the left end bar 8, the operator proceeds to align, in a column immediately to the right of the reading guide, the first twenty-five letters of the message. This is most conveniently done by placing the eraser end of a pencil upon the successive desired letters as found on the successive alphabet strips 4 from the top downwards, and pulling or pushing the alphabet strips in their channel ways toward the reading guide so that each strip stops with the proper letter just to the right of the right-hand edge of

the reading guide 5. When the alphabet strips are being aligned on the left-hand side of the device, as in the above procedure, the operator confines his search for letters to the left-hand half of the duplicated sequence on each alphabet strip.

When all twenty-five alphabet strips have been aligned as indicated, there is disclosed a multiplicity of columns of letters to the right of the plain-text column of letters thus aligned. All these columns of letters, except one, are columns of cipher letters, each column representing a cipher equivalent of the plain-text column. The single exception is the column which is the twenty-fifth removed from the plain-text column set up by the operator, and is merely a repetition of that plain-text column. One of these cipher columns is selected at random and is recorded in five-letter groups. The reading guide 5 is useful in this operation, since by placing it alongside the column selected, reading of the cipher column is facilitated. Suppose that the reading guide 5 be moved so that its left-hand edge aligns a column of cipher text. As shown in Fig. 4, such a column would read as follows:

SNAFJ LXRJG GVWVA ATVWW PVNUT

These letters are recorded and constitute the cipher letters for the twenty-five plain-text letters.

The reading guide 5 is now moved to the extreme right of the device, up against the right end bar 9; the next twenty-five letters of the plain text are aligned against the left edge of the reading guide 5. Again a set of columns of cipher letters are disclosed to the left of the reading guide. One of these columns is selected at random and again a set of twenty-five cipher letters representing the second set of twenty-five plain-text letters is recorded. If the message contains more than fifty letters, the foregoing procedure is repeated until the entire message has been enciphered. There is no need to indicate to the recipient of the message which column is selected for the cipher equivalent of each set of twenty-five plain-text letters, as will be noted presently.

To decipher the message, having the alphabets and the key according to which they have been arranged, the operator merely proceeds as in encipherment, aligning the alphabet strips in their channel ways so that the first twenty-five cipher letters of the cryptogram are in one column. He then examines all the other twenty-five columns of letters, looking for one which contains intelligible text throughout its extent from top to bottom. There will be one and only one such column, and this will be the plain-text equivalent of the column of cipher text set up on the device. The reading guide 5 is useful in this search for the plain-text column, as it can readly be moved to scan the successive columns from left to right, or from right to left. The plain-text column thus found is recorded in word lengths and the operator proceeds to set up the next twenty-five cipher letters on the right-hand side of the device. Again he looks for a plain-text column and records it when found. He continues this process until the message has been completely deciphered.

In the form of invention shown in Fig. 2, the device comprises a pair of hinged components F—F' of metal, Bakelite or other suitable material and foldable on one another in the manner of a book. As here shown, the grooved slideways 3 are formed on the inner faces of the said components by milling, or in the case where a condensation product such as Bakelite is used, may be molded in the material. In the embodiment disclosed, there are a total of thirty such slideways, fifteen in each component, though it will be understood that the invention is not limited to any particular number. It will be noted that the slideways are open at their opposite ends so that the alphabet strips may be readily inserted and freely extended outwardly therefrom as they are slid into different positions in the operations of enciphering and deciphering. As in other forms of the invention, a T-grip 6 is attached to the guide rule 5 at its end for the purpose of manipulating the rule, and is slidable in a channel 20 having therein undercut grooves 21 and 22 formed laterally along its inside edges. The grip 6 is provided with a spring-pressed element 23 engaging in bottom groove 21, and having an oppositely disposed bead 24 engaging in the opposite groove 22 whereby the grip 6 is maintained under suitable sliding tension in the channel 20, and whereby the guide rule 5 is manipulated transversely in relation to the alphabet strips 4; and the opposite end of the rule is adapted to slide freely in a lateral undercut groove 25 formed in component F'. The grip 6 is rigidly secured to the guide rule 5 in the manner of a T-square and may be so manipulated that the rule affords a positive means of obtaining an accurate alignment in column formation of the characters on said alphabet strips and in varying relations for cryptographic purposes. This foldable form of device presents a number of practical advantages, among which may be mentioned its compactness and portability; also the foldable feature permits exclusion of dust and dirt.

While in one form of device here disclosed, cylindrical rods are secured to a base at regular intervals from one another to form the channel ways into which the alphabet strips are inserted, it should be understood that any other means may be employed to form the channel ways. For example, a series of elongated metal strips known in the trade as "card holders," used ordinarily to hold narrow strips of paper bearing names of mail-box owners in apartment houses, etc., may be used to form the channel ways; these card holders may be riveted to the base, or spot welded to it, or attached in any other suitable manner. Or as disclosed in connection with Fig. 2, the channel ways may be formed by milling grooves in the base 1 itself, which may be made of molded Bakelite, for example. In such case the grooves are made by a rotating cutter which undercuts at the two edges, forming a channel way such as is commonly found in slide-rules. Figure 6 shows such a section in the form of a piece of Bakelite or similar material 13, in which five such channel ways 3 have been cut. Sections with equal or unequal numbers of channel ways may be easily provided and given identifying symbols such as letters, A, B, C, . . .

In Fig. 7 there is shown a sub-base suitable for use with such sections of channel ways. Thus, instead of having all the channel ways on a single base, as is the case in Fig. 1, the sub-base is merely made in the form of a flat surface onto which sections of channel ways may be positioned and temporarily fixed, so that rearrangements of sections can be made according to subsidiary keys. Referring to Fig. 7, the sub-base 1a is a plane

surface which is provided with an undercut slot 14, for carrying a sliding clamp 15, provided with a knurled thumb screw 16, for fastening the clamp into position. End bars 8 and 9 elevated above the base by supports 17 and back stop 18, serve the same purpose as similarly designated end bars of Fig. 1.

Using a sub-base such as that shown in Fig. 7, with several sections such as that shown in Fig. 6, one method of operation of this embodiment of the invention is shown in Fig. 5. In that figure there are five sections of 3, 4, 5, 7 and 8 channel ways, giving a total of twenty-seven channel ways. First, the sections are temporarily fastened to the base in the alphabetical order of their identifying symbols. Then the twenty-seven alphabet strips would be inserted in the twenty-seven consecutive channel ways according to the predetermined numerical key already referred to above in connection with Fig. 1. To encipher a given message, there would then be a subsidiary or specific key, also arranged for in advance by means of an indicator in the message, which would direct that the sections be now placed onto the base in a mixed order, say E—D—A—B—C, as shown in Fig. 5. The encipherment of a message would then proceed exactly as before. In another message, the indicator for the sectional arrangement might be different, say one calling for the sequence of sections D—A—C—E—B. Thus, with five sections there could be 120 different arrangements of sections on the base, even though only one set of alphabet strips is employed. The purpose of this is, of course, to increase the keying possibilities of the device, and to impart uniqueness to successive messages, without going to the trouble of making a complete rearrangement of all alphabet strips in the set of twenty-five channel ways.

The many uses of this device, with variable alphabets, in crytographic or cryptanalytic studies will be apparent to all skilled in the art and nothing further need be said on this score except that there has existed for many years a hitherto unfulfilled need for a simple device of this type, suitable for the insertion of sliding alphabets.

Changes, modifications and equivalent arrangements are contemplated within the scope of the invention as defined by the appended claims.

I claim:

1. A cryptographic device comprising a base provided with a plurality of horizontal channel ways; strips provided with discrete sequences of equally spaced alphabetic characters adapted for insertion therein and adjustable independently of one another and means for facilitating the reading of said characters in selected columns.

2. A cryptographic device comprising a base, said base being provided with a plurality of vertical channel ways, and individually adjustable strips bearing discrete sequences of equally spaced alphabetic characters adapted to be slidably inserted therein; and means for facilitating the reading of said characters in selected columns and in different relations for cryptographic purposes.

3. A cryptographic device comprising a base formed with horizontally grooved slide-ways therein; individually adjustable alphabetic strips slidable in said ways; and means to facilitate the reading of selected alphabetic columns in varying relations for cryptographic purposes.

4. A cryptographic device comprising a base formed with grooved slide-ways therein; strips bearing thereon alphabetic character sequences and individually movable in said ways; and means adjustable transversely of said strips to facilitate the reading of said characters in varying relations for enciphering and deciphering messages.

5. A cryptographic device comprising a base having vertically grooved slide-ways formed therein; strips bearing thereon alphabetic character sequences and individually slidable in said ways; and means adjustable transversely of said strips for facilitating the reading of said characters in varying relations for enciphering and deciphering messages.

6. A cryptographic device comprising a base provided with a plurality of channel ways; alphabet bearing strips adapted to be individually inserted and aligned in varying relations in said ways for cryptographic purposes; and a slidable guide rule for making excursions transversely along the channel ways and in relation to said strips for enciphering and deciphering messages.

7. A cryptographic device comprising a base having a supporting foot hingedly attached to the under surface of said base; a plurality of members fixed to the obverse surface of the base at equidistant intervals to form a plurality of channel ways; strips bearing alphabetic sequences of characters individually slidable in said ways; a guide rule adapted to be moved transversely of said strips to facilitate the reading of selected sequences of characters in varying relations for cryptographic purposes; and stop members for the guide rule disposed at opposite ends of said channel ways.

8. A cryptographic device comprising a sub-base; interchangeable base-sections having grooves formed therein to provide a plurality of channel ways; means for removably attaching said sections in position on said sub-base to permit different arrangements of said sections in juxtaposed relationship for cryptographic purposes; character bearing strips adapted for slidable insertion in said channel ways; and a slidable guide rule movable transversely across said channel ways and in varying relations to said strips for enciphering and deciphering messages.

9. A combination according to claim 8 in which said grooved sections are of the same size and contain equal numbers of channel ways.

10. A combination according to claim 8, in which said grooved sections are of different sizes and contain unequal numbers of channel ways.

11. A combination according to claim 8 in which stops are provided at the opposite ends of the channel ways to limit the movement of the slide rule at the end of its travel.

12. A cryptographic device comprising a frame structure and including a sub-base formed therein; a series of base-sections having grooves therein to provide a plurality of channel ways; means for removably attaching said sections on said sub-base to permit different juxtaposed arrangements thereof for cryptographic purposes; strips bearing alphabetic sequences of characters slidable in said ways; and a slidable guide rule movable transversely of said strips and alignable in varying relations with respect to said characters for enciphering and deciphering messages.

13. A cryptographic device comprising a frame structure and including a sub-base therein; base-sections grooved to provide a plurality of channel ways, said sections having different numbers of said channel ways and being differentiated from one another by distinguishing symbols; means for detachably securing said sections

on the sub-base to permit different juxtaposed arrangements thereof for cryptographic purposes; strips bearing alphabetic sequences of characters movable in said channel ways; a guide rule slidable transversely of said strips and alignable in varying relations with said characters for enciphering and deciphering messages; and stop members at opposite ends of the channel ways to limit the movement of the slide rule at the end of its travel.

14. A cryptographic device comprising a multiple base formed of separate sections, said sections being interchangeable with one another to permit different juxtaposed arrangements for cryptographic purposes; a plurality of channel ways in said sections; strips bearing sequences of characters and individually slidable in said ways; and a guide rule movable transversely of said strips and alignable with said characters in varying relations for enciphering and deciphering messages.

15. A cryptographic device including a multiform base composed of separate sections, said sections having grooved slide-ways therein and being interchangeable with one another to permit different juxtaposed arrangements for cryptographic purposes; strips slidable in said ways and bearing thereon sequences of alphabetic characters; and guide means disposed transversely of said strips and movable to facilitate alignment of the characters in varying relations for enciphering and deciphering messages.

16. A cryptographic device composed of hinged sections foldable upon one another, said sections having grooved slide-ways formed on their inner faces; strips slidable in said ways and bearing thereon sequences of alphabetic characters; and guide means disposed transversely of said strips and movable to facilitate alignment of the characters in varying relations for enciphering and deciphering messages.

17. A cryptographic device composed of hinged sections foldable upon one another, said sections being provided on their inner faces with open-ended slide ways; strips slidable in said ways and bearing thereon sequences of alphabetic characters; and a guide rule hinged to fold with said sections, said rule being disposed transversely of said strips and movable to facilitate reading of the characters in varying relations for enciphering and deciphering messages.

18. A cryptographic device comprising a pair of hinged components foldable upon one another, said components being provided on their inner faces with open-ended slide ways; a guide rule hinged to fold with said components; means operative with one of said components to maintain said rule in a position transversely of said strips and movable to facilitate reading of the characters in column formation and in varying relations for enciphering and deciphering messages; and terminal stops to limit the movements of said rule at either end of its travel.

19. A cryptographic device comprising hinged components foldable upon one another, said components being provided on their inner faces with a plurality of slide ways; a guide rule hinged to fold with said components; a grooved channel formed along the edge of one of said components in parallelism with the slide ways; means including a spring-tensioned element slidable in said channel for operating the said rule while maintaining the same in a position transversely of said strips, said rule being movable to facilitate reading of the characters in varying relations and in column formation for enciphering and deciphering messages.

WILLIAM F. FRIEDMAN.

March 5, 1946. W. F. FRIEDMAN 2,395,863

CRYPTOGRAPHIC DEVICE

Filed Oct. 19, 1939 3 Sheets-Sheet 3

FIG. 6.

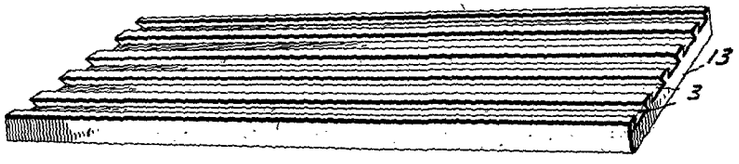
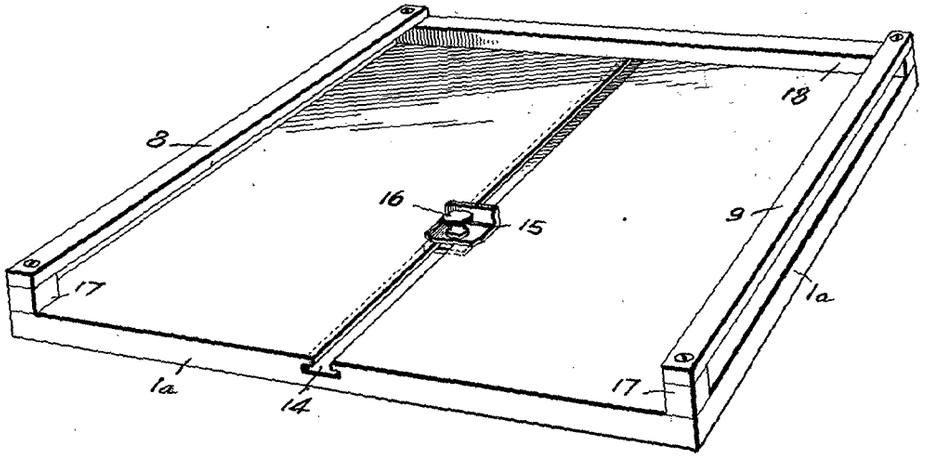


FIG. 7.



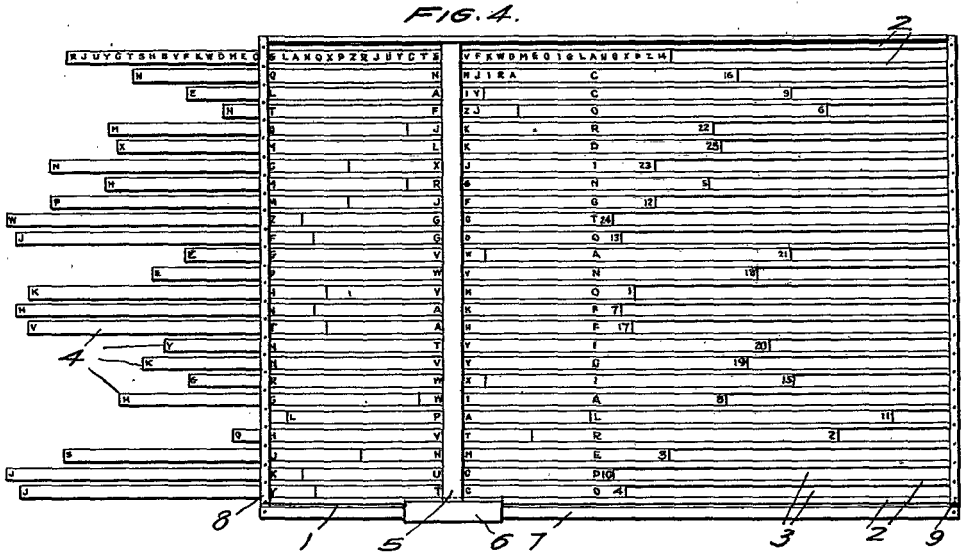
INVENTOR
WILLIAM F. FRIEDMAN
BY Edgar H. Ingram
Charles A. Rowe
ATTORNEYS

March 5, 1946. W. F. FRIEDMAN 2,395,863

CRYPTOGRAPHIC DEVICE

Filed Oct. 19, 1939 3 Sheets-Sheet 2

FIG. 4.



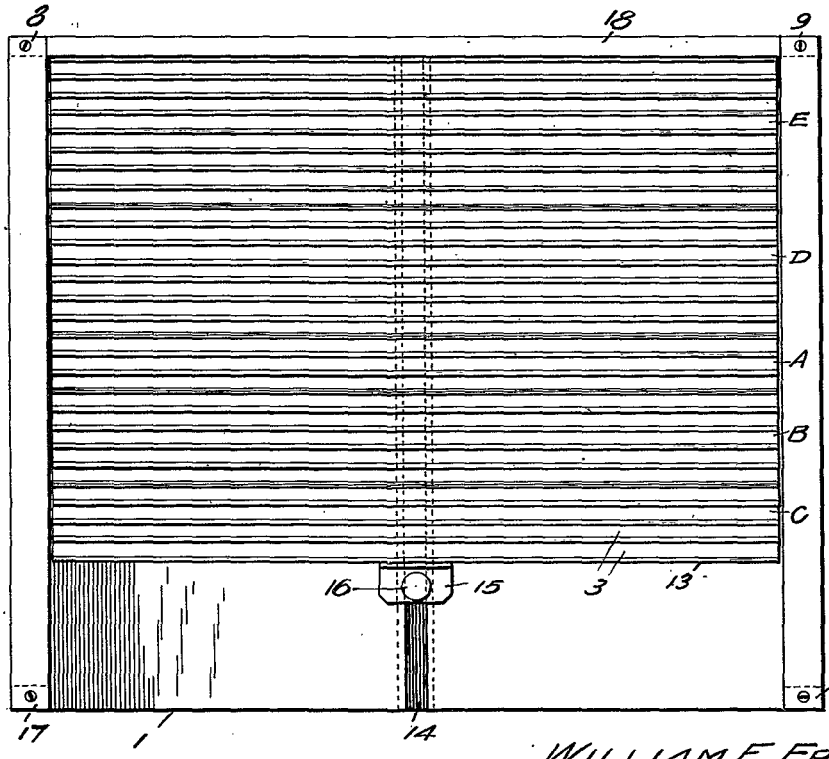


FIG. 5.

INVENTOR
WILLIAM F. FRIEDMAN
By Edgar H. Snodgrass
Charles A. Rowe
ATTORNEYS

March 5, 1946. W. F. FRIEDMAN 2,395,863

CRYPTOGRAPHIC DEVICE

Filed Oct. 19, 1939 3 Sheets-Sheet 1

FIG. 1.

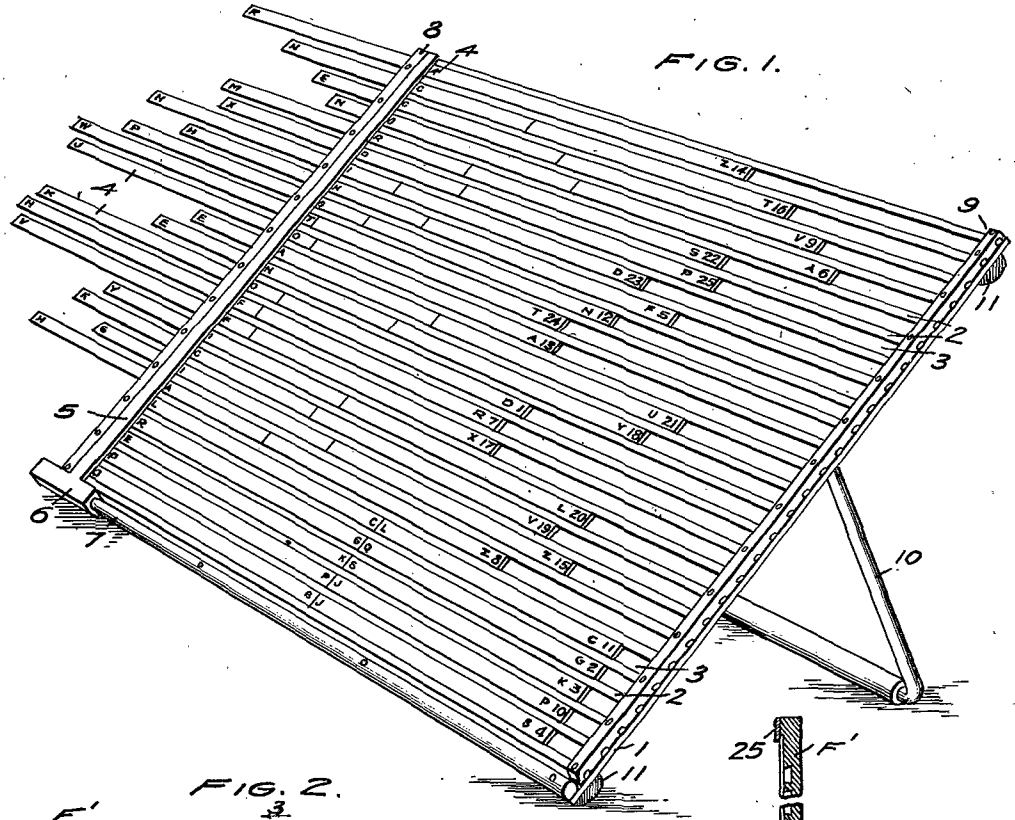


FIG. 2.

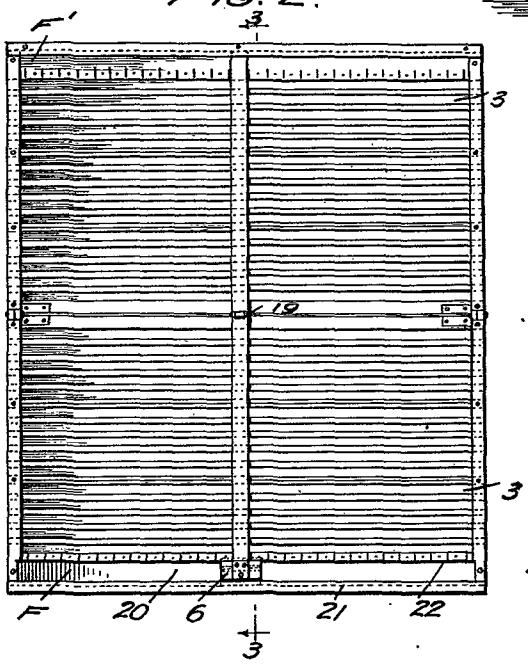


FIG. 3.

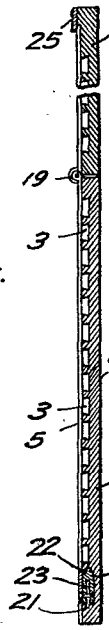
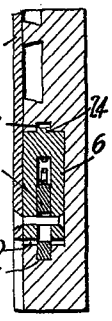


FIG. 3a.



INVENTOR
WILLIAM F. FRIEDMAN
BY Elgar H. Snodgrass
Charles A. Rowe
ATTORNEYS